DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

MCO 3501.36
PS

MARINE CORPS ORDER 3501.36

From: Commandant of the Marine Corps
To: Distribution List

Subj: MARINE CORPS CRITICAL INFRASTRUCTURE PROTECTION (MCCIP) PROGRAM

Ref: (a) HSPD 7, “Critical Infrastructure Identification,” December 17, 2003
(b) PDD 63, “Critical Infrastructure Protection,” May 22, 1998
(c) DoD CIP Plan, November 18, 1998
(d) DoDD 8500.1, “Information Assurance,” October 24, 2002
(e) DoDI 8500.2, “Information Assurance Implementation,” February 6, 2003
(f) CJCSI 6510.01C, “Information Assurance and Computer Network Defense,” May 1, 2001
(g) SECNAVINST 3501.1, “Critical Infrastructure Protection (CIP),” June 16, 2002
(h) DON Consequence Management Planning Guide, December 2002
(i) MCO 5239.2, “Information Assurance Program,” November 18, 2002
(j) DoDD 5000.1, “The Defense Acquisition System,” May 12, 2003
(k) DoDI 5000.2, “Operation of the Defense Acquisition System,” May 12, 2003
(l) United States Code Title 10, Subtitle C, Chapter 506, August 10, 1956
(m) Public Health Security Bioterrorism Preparedness and Response Act of 2002, June 12, 2002
(n) DoDI 3020.39, “Defense Intelligence Continuity of Operations,” August 3, 2001
(o) MCO 3302.1D, “The Marine Corps Antiterrorism/Force Protection (AT/FP) Program,” July 12, 2002
(p) MC Installation CBRNE Preparedness Campaign Plan, December 1, 2003
(q) DoD O-2000.12H Antiterrorism Handbook, February 9, 2004

Encl: (1) Critical Infrastructure Protection Terms
(2) Critical Infrastructure Protection Definitions

1. Situation. To establish policies, procedures, and responsibilities for the development and implementation of a MCCIP Program.

2. Mission

a. The Marine Corps shall identify, protect, and ensure the availability of those assets and infrastructures critical to the execution of its mission. In doing so, our efforts must recognize that mission assurance is highly dependent upon both USMC and non-USMC assets and infrastructures.

b. Critical Infrastructure Protection (CIP) Program efforts encompass all aspects of operational security, physical security, infrastructure assurance, information assurance (IA), information security, and antiterrorism as provided in references (a) thru (o). Reference (p), addresses the issue of asymmetric threats to include the use of weapons of mass destruction, information warfare, and CBRNE. The CIP Program compliments the AT/FP Program to provide mission assurance and personnel protection. The number of references sited in the AT/FP Marine Corps Order 3302.1D provides additional guidance in order to execute the CIP Program. The CIP Program is designed to support overall mission assurance, and as such, is considered a critical element in acquisition and operations planning. As stated within the CBRNE Campaign Plan, the objectives for supporting installation CBRNE defense is to provide the appropriate level of protection to support mission continuity as referenced in (p). The CIP Program is designed to support and compliment the overall objectives as contained in the CBRNE Campaign Plan.

c. A key aspect of the CIP Program is to support combatant commander (COCOM) plans. The effort to ensure that critical infrastructure is identified and protected against loss or significant degradation is an interagency effort by the Marine Corps, the Department of Defense (DOD), Federal and state agencies, and local civilian and

government agencies. The Marine Corps will establish and maintain a CIP Program that shall:

(1) Support national and DoD CIP requirements.

(2) Identify critical capabilities, assets, and infrastructures that support warfighting operational requirements.

(3) Coordinate CIP Program efforts with COCOMs, DoD agencies, and other Services.

(4) Develop a formal methodology to track and inform COCOMs, DoD agencies, and other Services regarding Service CIP risk management decisions that affect COCOM plans or vital Marine Corps missions.

(5) Incorporate CIP into all Service planning and associated exercise processes.

(6) Identify and prioritize Service CIP requirements as part of the Program Planning Budgeting and Execution cycle.

(7) Identify joint mission essential tasks (JMET) or capabilities that directly support COCOM OPLANs, by implementing and conducting mission area analysis that identify and assess assets and infrastructures that are critical to the execution of assigned OPLANs.

3. Execution. The references provide policy, procedures, and guidance for the MCCIP Program. Further information is available on http://hqinet001.hqmc.usmc.mil/pp&o/ps/PSC_Critical_Infrastructure_Assurance_Branch/CIP/References/Reference_home.html. Future Department of Defense and Marine Corps directives will provide guidance to identify and protect our Nation’s critical assets. The identification and protection of critical assets are accomplished by implementing a continuous six-step activity or event cycle management process. The six-steps are infrastructure analysis and assessment, remediation, monitoring and reporting, mitigation, response, and reconstitution. This process evaluates activities that occur before, during, and after an event that could result in infrastructure being compromised, disrupted, or destroyed. An integral part of this process is recognizing the interdependencies between Marine Corps, DoD, and

commercial assets and infrastructures; and their collective impact on mission execution. The enclosures provide additional information.

a. Commandant's Intent and Concept of Operations

(1) Commandant's Intent for MCCIP Program. Identify, protect, and ensure the availability of infrastructures, assets, and capabilities deemed critical to Marine Corps forces in accomplishing their warfighting mission, and plan to mitigate the effects of their potential loss or disruption.

(2) Concept of Operations. To identify, assess, and protect Marine Corps assets and infrastructures deemed critical to the execution of warfighter mission(s). This will be accomplished through a continuous six-step event management process. Reference q is provided as a source to assist in conducting various analysis and assessments. This process must incorporate the following analysis and risk management tasks:

(a) Identify critical/key assets to be protected, and review the impact to the mission if those assets were lost or disrupted. Review both USMC and non-USMC assets.

(b) Value and prioritize assets based on consequences to mission(s) if lost.

(c) Conduct a threat analysis and assessment. Identify threats, hazards (natural and man-made), and other undesirable events to which each critical asset is exposed. Assess the probability of occurrence and the expected impact of each threat on each asset.

(d) Perform a vulnerability analysis and assessment. Analyze vulnerabilities of each critical asset to each identified threat and hazard. Assess the probability of a threat or hazard occurring and determine the adequacy of existing security measures, identify deficiencies, evaluate alternatives, and verify the adequacy of implemented security measures.

(e) Conduct an analytical risk assessment to determine the priorities for critical asset protection and

identify unacceptable risks and risk remediation priorities.

(f) Identify remediation and countermeasure recommendations as well as the associated costs, and prioritize by cost benefit analysis.

(g) Prioritize the countermeasure and remediation options that address identified risks.

b. Organizational Responsibilities

(1) The Commandant of the Marine Corps (CMC). The CMC executes the coordination of the MCCIP Program through the appointment of the following:

(a) Deputy Commandant for Plans, Policies and Operations (DC, PP&O), shall:

1. Have overall responsibility for the development, implementation, and execution of CIP policy within the Marine Corps.

2. Represent the Marine Corps on the Department of the Navy's Critical Infrastructure Assurance Office (DON CIAO) Council and provide membership to the DoD Critical Infrastructure Protection Integration Staff (CIPIS).

3. Oversee MCCIP Program initiatives and coordinate these activities with the DON.

4. Chair the Headquarters Marine Corps Critical Infrastructure Protection Working Group (HQMC CIPWG).

5. Serve as the advocate and central point of contact for MCCIP Program related issues, to include establishing and maintaining a secure and compatible relational database management system.

6. Provide oversight for Integrated Vulnerability Assessments conducted on Marine Corps installations, bases, and areas of interest.

7. Serve as the liaison between HQMC and the MARFOR in initiating, developing, and implementing

uniform and standardized assistance in CIP education, training, exercises, policies, procedures, and methodologies to be implemented at the MARFOR level.

8. Serve as liaison and point of contact between HQMC and the COCOMs, via the cognizant MARFOR component command for MCCIP Program requirements in enclosure (1).

9. Represent the Marine Corps in joint DoD efforts pertaining to the standardization and uniform application of various CIP Program requirements and methodologies.

10. Serve as the original classification authority for the MCCIP Program.

11. Will be responsible for the submission of all CIP funding requests to the DPO-MA.

12. The CIP Program is currently a program of record at HQMC. With funding in core through the Fiscal Year Develop Program (FYDP). Funding is for program management only and not for vulnerability remediation. As in AT/FP, CIP vulnerability remediation must be funded through the Program Objective Memorandum (POM) process. It will be the responsibility of the MARFORs and installations to secure funding through base operations funding.

(b) Commanding General, Marine Corps Combat Development Command (CG, MCCDC) shall:

1. Develop CIP/AT/FP doctrinal requirements, procedures, and/or guidance for base and installation commanders for the identification, assessment, protection options; and management of risks associated with critical commercial infrastructure vulnerabilities and dependencies.

2. Validate Marine Corps CIP requirements to DC, PP&O.

3. Ensure Marine Corps IA requirements are incorporated into all acquisition and investment requirements documents.

4. Ensure CIP concepts are incorporated into Marine Corps systems architecture that contains an information technology (IT) component in order to meet current DoD, DON, and Marine Corps IA specifications.

(c) Deputy Commandant for Manpower & Reserve Affairs (DC, M&RA) shall:

1. Serve as the sector lead for all CIP Manpower plans, classification, and assignment related matters.

2. Identify and rank critical, Marine Corps -owned and -managed personnel management IT systems that have single points of entry/access and may be vulnerable to attack (electronic or physical).

3. Participate in the conduct of integrated vulnerability assessments on Marine Corps critical personnel management IT systems that have single points of entry/access.

4. Develop CIP sensitive procedures for the remediation, mitigation, and assurance that the minimum essential level of personnel management can be protected, maintained, or replicated.

5. Coordinate with DC, PP&O to identify and seek the required personnel structure and staffing to fully support CIP requirements.

6. Serve as a member of the HQMC CIPWG.

(d) Deputy Commandant for Programs and Resources (DC, P&R) shall:

1. Serve as the advocate for CIP funding and resources. Coordinate with DC, PP&O to identify near-, mid-, and long-term CIP funding sources and opportunities.

2. Serve as the financial sector lead for CIP funding and resource issues, and as a member of the HQMC CIPWG.

(e) Director, Command, Control, Communications, and Computers (Dir, C4) shall:

1. Develop and maintain a set of standard Marine Corps Enterprise Network (MCEN) IA requirements for inclusion in all Marine Corps acquisition and investment requirements documents, as well as service and sole source contracts. At a minimum, this document shall identify the MCENs requirements for security certification and accreditation, joint interoperability, electromagnetic environmental effects, and spectrum management requirements.

2. Approve, explicitly identify, and maintain a repository of IA mission assurance category (MAC) levels and confidentiality levels for all Marine Corps systems.

3. Support DC, PP&O in the technical evaluation and MCEN compatibility of command and control (C2) systems designed to provide real-time CIP, AT/FP situational awareness, threat monitoring, and reporting and coordinated security force response activity.

4. In coordination with DC, PP&O, assist with the evaluation, certification, and implementation of the Marine Corps CIP database on the MCEN.

5. Provide IA/policy support to the HQMC CIPWG.

(f) Deputy Commandant for Installations and Logistics (DC, I&L) shall:

1. Provide guidance and strategic direction for the relocation of Marine Corps mission critical assets from civilian-shared tenant spaces into secured-Marine Corps or –Government facilities with appropriate physical security.

2. Ensure that Marine Corps IA requirements are incorporated into all acquisition investment requirements documents.

3. Provide representation to the HQMC CIPWG.

4. Analyze, address, and provide support for infrastructure protection of critical maintenance, supply and logistics processes, facilities, and assets.

5. Develop and implement physical security structural upgrade programs for existing facilities housing mission critical assets.

6. In coordination with DC, PP&O and Dir, C4, analyze, develop and implement a standardized, uniform geospatial information system capability that can be utilized:

a. within the framework of a real-time, common operational picture system with respect to CIP, AT/FP, and installation chemical, biological, radiological, nuclear, and high yield explosives defense posture, threat monitoring, reporting and decision support, and coordinated security force planning and response activity; and

b. within the framework of the Marine Corps CIP relational database management system.

7. Ensure compliance with enclosure (1) as amended.

8. Provide doctrine and guidance for installation and bases for establishing and implementing mutual aid, assistance, and support for joint military-civilian emergency response activities.

(g) Director for Intelligence shall:

1. Support the evaluation and development of technology initiatives for an integrated indications and warning capability.

2. Support PP&O and C4 in the technical evaluation and MCEN compatibility of intelligence systems designed to provide real-time AT/FP intelligence, analysis, threat monitoring, and reporting.

3. Provide intelligence support to threat analysis and assessment, through the Marine Corps Intelligence Activity (MCIA), to PP&O and MARFOR in order to identify threats, hazards (natural and man-made), and other undesirable events to which a critical asset may be exposed. Assist in assessing the probability of occurrence and the expected impact of each threat on each asset.

4. Appoint a member to defense and national intelligence community continuity of operations working groups to represent Marine Corps intelligence equities in compliance with enclosure (1). Apprise the CMC of the status and quality of national and defense intelligence agencies CIP preparedness.

5. Ensure that Marine Corps IA requirements are incorporated into the acquisition requirements documents for intelligence systems.

6. Serve as a member of the HQMC CIPWG.

(h) The Inspector General of the Marine Corps (IGMC) shall:

1. Coordinate with the DC, PP&O (PS) regarding integration of the provisions of this Order into the Automated Inspection Reporting System checklist.

2. Conduct reviews as part of the Marine Corps command inspection programs to determine compliance with the requirements contained in this Order.

(i) Commanding General, Training and Education Command (TECOM) shall:

1. Coordinate with existing interservice antiterrorism officer courses to develop and incorporate CIP training into existing curriculum.

2. Coordinate CIP development and training programs with PP&O and Government agencies responsible for standardization of the CIP Program development.

3. Develop and implement CIP education and training requirements into commissioned officer, warrant officer, and staff non-commissioned officer professional military education programs, and where applicable and appropriate, incorporate CIP training into existing formal schools and/or courses.

4. Provide support to DC, PP&O in developing CIP self-assessments tools.

5. Develop CIP and AT/FP distance learning education products (computer-based training, Marine Corps Institute courses) in order to maximize wider awareness and understanding across the total force.

6. Serve as a member of the HQMC CIPWG.

(j) Commanding Officer, Marine Corps Operational Test and Evaluation Activity (MCOTEA) shall:

1. Develop and incorporate CIP evaluation into the Test and Evaluation Master Plan and Test and Integration Working Group process.

2. Evaluate IA protection, detection, reaction, and response mechanisms as a function of MAC and confidentiality levels during operational test and evaluation.

3. Evaluate CIP impacts of security certification and accreditation, joint interoperability, electromagnetic environmental effects, and spectrum management as requirements when appropriate.

4. Provide representation to the HQMC, CIPWG.

(k) Director, Health Services shall:

1. Serve as the sector lead for health services and a member of the HQMC CIPWG.

2. Undertake action to ensure the security, privacy, and survivability of health records and data.

3. Participate in the conduct of integrated vulnerability assessments as related to health services systems. Identify critical medical assets on installations and throughout the Marine Corps.

4. Coordinate with Bureau of Medicine and Surgery (BUMED), Office of Homeland Security, regarding the support from Navy Medical Treatment Facilities (MTF) to ensure the abilities of medical assets and infrastructure critical to the execution of the mission(s) are maintained and are fully capable.

(l) Commanding Officer, Marine Corps Network Operations Support Command shall:

1. Evaluate the survivability and security of the MCEN, and protect against system degradation or loss.

2. Provide resources to support MCOTEA in its evaluation of the protection mechanism of fielded systems as part of the operational test and evaluation process.

(m) Commanding Officer, Marine Corps Systems Command (MCSC) shall:

1. Provide resources through the Marine Corps Tactical Systems Support Activity (MCTSSA) to ensure that security certification and accreditation, joint interoperability, electromagnetic survivability and compatibility, and spectrum allocation and assignment are validated as part of the developmental test and evaluation of new Marine Corps systems.

2. Maintain a repository of proposed and approved MACs for all legacy and developmental Marine Corps programs.

3. Embed and integrate CIP concepts which assess such issues as single points of service or single points of manufacture in defense industrial base programs and products, in connection with developing, acquiring, and fielding material solutions to support requirements for the operating forces, bases, and installations.

(n) Staff Judge Advocate (SJA) to the Commandant of the Marine Corps shall:

1. Conduct legal reviews of CIP plans, operations, exercises (including but not limited to force/rules of engagement), for compliance with domestic and international law, and provide legal advice on the establishment of joint military-civilian efforts to protect both critical military and commercial assets upon which military operations are dependent, and on the development of joint mutual aid and assistance agreements for joint military-civilian emergency response activities.

2. Provide representation to the HQMC CIPWG.

c. Command Responsibilities. Commanding generals/officers are responsible for the overall management of CIP programs for all assets within their purview. Commanders will develop, implement, and maintain effective CIP plans in order to ensure that the physical and cyber critical infrastructure and assets on which the Marine Corps depends are available to mobilize, deploy, and sustain military operations. In the event of degradation or complete failure of key critical infrastructure and assets, commanders shall ensure plans address appropriate mitigation strategies. The commanding generals/officers shall:

(1) Protect infrastructure and assets under their purview deemed critical to mission execution; protect material readiness and operations in peace, crisis, and war; plan to mitigate the effects of the loss of disruption of mission critical assets; and the timely restoration or recovery of those critical assets.

(2) Recognize that Marine Corps equipment, facilities, utilities, services, weapon systems, and mission accomplishment are highly dependent upon non-DoD assets, including national/international infrastructures, facilities and services of the private sector, and other Government departments and agencies. As a result, threat and vulnerability analyses are critical for success to the MCCIP Program.

(3) Develop, implement, and maintain effective CIP programs utilizing the six-step event management process.

(4) Incorporate CIP exercise planning and training into CIP programs for both USMC and non-USMC assets.

(5) Observe, report, and propose administrative action to the next level of command required for the protection of Marine Corps and non-Marine Corps infrastructures and assets. In those cases where security of non-Marine Corps assets rests primarily with commercial or non-military asset owners, or with local, state, Federal and/or foreign national authorities, it is the commander’s responsibility to notify such asset owners of identified

vulnerabilities and to request the asset owner to voluntarily undertake appropriate remediation activities.

(6) Increase awareness of the CIP Program through information sharing, training and education, and cooperative agreements and outreach with the private sectors.

(7) Determine and manage the risk to mission-critical assets, systems, and processes supporting logistics and acquisition. Non-organic infrastructures and services that serve as sole source producers/single nodes of vulnerability in the manufacture and delivery of critical products and in providing support for operational sustainment, must be subjected to rigorous risk assessment analysis, leading to an acceptable risk management plan. With respect to risk management decisions affecting assets that are critical to the execution of JMETLs that support assigned OPLANs those decisions must be communicated via Naval message to the CIP cognizant MARFOR CIP component, who shall review and evaluate the risk management decision. The CIP cognizant MARFOR component shall then communicate the risk management decision to the appropriate COCOM.

(8) Use the results of the various analyses performed under the CIP Program (such as the risk analysis and linking critical assets to JMETLs) to support the determination of needed funding, to establish remediation and mitigation priorities and thus funding priorities, and to procure resources and obtain approval of actions.

(9) Establish and implement mutual aid, assistance and support for joint military-civilian emergency response activities.

(10) At the MARFOR level of command:

(a) Implement, administer, and manage the CIP database functions and requirements in conjunction with the COCOMs and with HQMC.

(b) The CIP database shall provide continuous support to both operational CIP taskings and the CIP six-step event management process. The MARFORS are required to update the relational database simultaneously with changes in the operational status of critical infrastructures or assets that support assigned missions.

(c) The MARFOR level will monitor and help to facilitate mutual aid, assistance and support for joint military-civilian emergency response activities.

(d) Provide doctrine and guidance for Reserve Training Centers for establishing and implementing mutual aid, assistance, and support for joint military-civilian emergency response activities.

(e) Incorporate CIP and AT/FP security requirements in the acquisition and procurement process.

4. Administration and Logistics

a. Recommendations for changes to this Order should be submitted to DC, PP&O via the appropriate chain-of-command.

b. Future guidance will be disseminated via Operational Standards documents, which will provide guidance for CIP programs, concepts, and methodologies. The operational standards will be made available via electronic transmission.

5. Command and Signal

a. Signal. This Order is effective the date signed.

b. Command. This Order is applicable to the Marine Corps Total Force.

J. C. Huly
Deputy Commandant for
Plans, Policies, and Operations

DISTRIBUTION: PCN 10203359100

Copy to: 7000260 (2)
8145001 (1)

ACRONYMS

Acronym	Term
A&A	Analysis and Assessment
ADUSD	Assistant Deputy Under Secretary of Defense
AOR	Area of Responsibility
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
AT&L	Acquisition, Technology and Logistics
AT/FP	Antiterrorism/Force Protection
BSA	Balanced Survivability Assessment
BUMED	Bureau of Medicine and Surgery
C2	Command and Control
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
CAL	Critical Asset List
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosives
CBT	Computer-Based Training
CERT	Computer Emergency Response Team
CI	Counter Intelligence
CIAO	Critical Infrastructure Assurance Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPLOG Database	Critical Infrastructure Protection Logistics Database
CIPIS	Critical Infrastructure Protection Integration Staff
CIRT	Computer Incident Response Team
CJCS	Chairman, Joint Chiefs of Staff
CNO	Chief of Naval Operations; also Computer Network Operations
CNOIVA	Chief of Naval Operations Integrated Vulnerability Assessment
COMSEC	Communications Security
CONPLAN	Concept Plan

Acronym	Term
CONUS	Continental United States
COOP	Continuity of Operations
CWS	Community Water Systems
DAA	Designated Approving Authority
DC/S	Deputy Chief of Staff
DC/S IL	Deputy Chief of Staff for Installations and Logistics
DC/S PP&O	Deputy Chief of Staff for Plans, Policy, and Operations
DI	Defense Infrastructure
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISAP	Defense Infrastructure Sector Assurance Plan
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DMS	Data Management System or Defense Message System
DOD	Department of Defense
DODD	DOD Directive
DODI	DOD Instruction
DON	Department of the Navy
DPAS	Defense Property Accountability System
DRU	Direct Reporting Unit
DSC	Defense Supply Center
DSN	Defense Stock Number
DTRA	Defense Threat Reduction Agency
DUSD(L&M)	Deputy Under Secretary of Defense (Logistics & Materiel)
DUSD(L&MR)	Deputy Under Secretary of Defense for Logistics And Materiel Readiness
EO	Executive Order
ER	Emergency Response
FISC	Fleet Industrial Supply Center
FIWC	Fleet Information Warfare Center
FOC	Full Operational Capability
FPCON	Force Protection Condition (formally THREATCOM, threat condition)
FY	Fiscal Year
GEOLOC	Geographical Location

Acronym	Term
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
GSA	General Services Administration
HQMC	Headquarters, U.S. Marine Corps
I&L	Installations and Logistics
I&W	Indications and Warnings
IA	Information Assurance
IAVA	Information Assurance Vulnerability Assessment; also, Information Assurance Vulnerability Alert
INFOCON	Information Operation Condition
INFOSEC	Information Security
INFOSYS	Information Systems
IR	Incident Response
IRT	Incident Response Team
IS	Information Security
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, and Reconnaissance
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IVA	Integrated Vulnerability Assessment
J-4	Joint Directorate (Logistics)
J-6	Joint Directorate (Information Systems)
JLC	Joint Logistics Commanders
JMETL	Joint Missions Essential Tasking List
LOC	Joint Logistics Operations Center
JPO-STC	Joint Program Office For Special Technology Countermeasures
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	Joint Task Force
JTF-CND	Joint Task Force — Computer Network Defense
JTF-CNO	Joint Task Force — Computer Network Operations
MAA	Mission area analysis

Acronym	Term
MAC	Mission Assurance Category
MAOC	Mission Assurance Operations Center (MAOC)
MARFORS	Marine Forces
MCAS	Marine Corps Air Station
MCEN	Marine Corps Enterprise Network
MCIA	Marine Corps Information Assurance
MCIVA	Marine Corps Integrated Vulnerability Assessment
MCLB	Marine Corps Logistics Base
MCOTEA	Marine Corps Operational Test and Evaluation Activity
MCSC	Marine Corps Systems Command
MCTSSA	Marine Corps Tactical Systems Support Activity
MER	Mission Essential Requirement
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
M & RA	Manpower & Reserve Affairs
MTAC	Multiple Threat Alert Center
MTF	Medical Treatment Facility
N4	Deputy Chief of Naval Operations for Fleet Readiness and Logistics
NAVCIRT	Naval Computer Incident Response Team
NETWARCOM	Navy Network Warfare Command
NCA	National Command Authority
NCIS	Naval Criminal Investigative Service
NDI	National Defense Infrastructure
NIPC	National Infrastructure Protection Center
NIPRNET	Non-Secure Internet Protocol Router Network
NMCC	National Military Command Center
NIVA	Naval Integrated Vulnerability Assessment
OASD	Office of the Assistant Secretary of Defense
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OCONUS	Out of Continental United States
OPLAN	Operations Plan
OPNAV	Chief of Naval Operations headquarters staff
PA&E	Program Analysis & Evaluation

Acronym	Term
PACOM	United States Pacific Command
PCCIP	President’s Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PE	Program Element
POA&M	Plan of Action and Milestones
POM	Program Objectives Memorandum
PPBES	Planning, Programming, & Budgeting Execution System
PP & O	Plans Programs and Operations
P & R	Programs and Resources
R&D	Research and Development
RUF/ROE	Rules for the Use of Force/Rules of Engagement
SBCCOM	Soldier And Biological Chemical Command
SDWA	Safe Drinking Water Act
SIPRNET	Secret Internet Protocol Router Network
SITREP	Situation Report
SJA	Staff Judge Advocate
SLA	Service Level Agreements
TECOM	Training and Education Command
TEMP TWIG	Test and Evaluation Master Plan and Test and Integration Working Group
THREATCOM	Threat Condition (replaced by FPCON, or Force Protection Condition)
TPFDD	Time-phased Force Deployment Data
USD	Under Secretary of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)	Under Secretary of Defense (Comptroller)
USMC	United States Marine Corps
USN	United States Navy
USNORTHCOM	U.S. Northern Command
USSPACECOM	U.S. Space Command
USTRANSCOM	U.S. Transportation Command
VA	Vulnerability Assessments

Critical Infrastructure Protection Terms and Definitions

Analysis and Assessment (A & A). The process used to identify and analyze critical assets, their associated infrastructures, interdependencies and single points of failure. The process also includes physical and cyber vulnerability assessments on the critical assets and interdependency related single points of failure.

Analysis (Infrastructure). Identifying infrastructure requirements to support DoD missions as well as a method of physically, logically, and operationally characterizing infrastructures as complex systems and assets.

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces (JP 1-02).

Assessment. (1) An objective evaluation of the vulnerabilities associated with Joint Force Capabilities. (2) An objective determination of how critical the capability and supporting infrastructure is in supporting military operations that accomplish the National Military Strategy. Focus is Combatant Command OPLANs. (3) A process to characterize the Department of Defense (DOD) infrastructures, their dependencies and interdependencies and subsequent linkages to commercial, foreign and host nation infrastructures.

Asset. Any military/governmental/private/commercial resource, relationship, instrument, installation, supply or system that in some combination is used in a military operational or support role. Assets are found at CONUS and OCONUS locations. Any infrastructure facility, equipment, service or resource that supports a DOD Component. A Critical Infrastructure Asset is an infrastructure asset deemed essential to DOD operations or the functioning of a Critical Asset. (DODD 5160.54) (DOD Plan – November 1998)

Assurance (Critical Capability/Infrastructure). Assurance is guarding against the loss or disruption of a critical capability/infrastructure. Assurance assumes the identification of capabilities, assets, nodes and infrastructures deemed critical to the DOD in peacetime, crisis and war. Assurance requires assessing potential threats and identifying potential actions to restore those capabilities, assets, nodes and

infrastructures (or functionality they provide) if they are lost, damaged, corrupted or compromised. Further, assurance requires identifying and resourcing options to protect, mitigate and improve the availability of these Critical Capabilities and Infrastructures that DOD organizations own, use, and control. The goal of assurance is to inform planners and decision makers of the probability of availability and quality (e.g., integrity, reliability, confidentiality, survivability, durability, capacity and adequacy) of specific capabilities and infrastructures. Examples of assurance activities are dedication of physical protection resources, development of redundant capability/means, and alteration of OPLANS and CONPLANS that depend on the identified capability in accepting the risks identified. (Enclosure (1) SECNAVINST 3501.1, 16 June 2002.) Assurance of a Critical Capability and/or Infrastructure is a shared responsibility. (DODD 5160.54) (DOD CIP Plan of November 1998)

Asymmetric Warfare. The attempts to circumvent or undermine a nation's strengths while exploiting its weaknesses by using methods other than conventional warfare, such as terrorism (physical and cyber), information warfare, space warfare and weapons of mass destruction.

Concept of Operations. A verbal or graphic statement, in broad outline, of a commander’s assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. It may also be referred to as commander’s concept or CONOPS. (JP 1-02)

Critical Asset/Critical Node/Critical Item (Critical Infrastructure).(1) An asset that can be either a DOD or non-DOD military-related unit, organization, facility/installation, system, resource, equipment or instrument that is identified as performing an essential service, function or use in military operational plans or in support of operational plans. (2) Any facility, equipment, service or resource considered essential to DOD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction and timely restoration. Critical Assets may be DOD assets or other government or private assets, domestic or foreign, whose disruption or loss would render DOD Critical Assets ineffective

or otherwise seriously disrupt DOD operations. Critical Assets include traditional physical facilities or equipment, non-physical assets (such as software systems) or assets that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

Critical Infrastructure. Those systems and assets essential to plan, mobilize, deploy and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the DOD to execute the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DODD 8500.1 (NOTAL))

Critical Infrastructure Protection (CIP). CIP is Mission Assurance. CIP is the identification, assessment, and assurance of cyber and physical infrastructures that support mission critical capabilities and requirements, to include the political, economic, technological and informational security environments essential to the execution of the National Military Strategy. (Joint Staff Definition used in coordinated response to Draft DODD 8500.1(NOTAL))

Criticality Index, Criticality Metric. Measurement established within an asset class, organization or sector, to assist in ranking assets for assurance or protection activities. An example would be a graduated indicator of impact from a system-wide slight degradation of service to cessation of operations. (Department of Defense Critical Asset Assurance Program Working Definition)

Criticality-Vulnerability Ratio. Comparison of criticality and vulnerability indices. (Department of Defense Critical Asset Assurance Program Working Definition)

Defense Infrastructure. Infrastructure owned, operated or provided by the Department of Defense. Defense infrastructure Sectors include the Defense Information Infrastructure (DII), Command/Control/Communications (C3), Space, Intelligence/ Surveillance/Reconnaissance (ISR), Financial Services, Logistics, Public Works (includes DOD owned or operated utilities, roads, rails and railheads and their interface to commercial and other government systems), Personnel, Health Affairs and Emergency Preparedness. (See also definitions of Infrastructure, National Infrastructure, National Defense Infrastructure, and International Defense Infrastructure.)

Denial/Degradation of Service and Assets. (1) A form of attack that reduces the availability of a resource. (2) An abnormal condition wherein the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact. (NP V 1.0)

Destruction of Asset/Infrastructure. A condition when the ability of a critical asset or infrastructure to provide its customers an expected level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero. (NP V 1.0)

Force Protection. Security program designed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replaces the existing term and its definition and is approved for inclusion in the next edition of Joint Pub 1-02.)

Information Assurance. (1) Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities and is also called IA. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02) (2) Information operations that protect key public and private elements of the national information infrastructure from exploitation, degradation and denial of service. (Modified from NSTAC)

Information Security. The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users. Information Security includes the measures necessary to detect, document and counter such threats. Information security is composed of computer security and communications security. It may also be referred to as INFOSEC. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This

term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

Information System. The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information. (Joint Publication 3-13, Joint Doctrine for Information Operations, 9 October 1998 – This term and its definition are approved for inclusion in the next edition of Joint Pub 1-02.)

Infrastructure. The framework of inter-dependent networks and systems comprising identifiable industries, institutions, functions and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole. (DoDD 5160.54) (DoD Plan – November 1998) (NP V 1 .0) (Bilateral Infrastructure – page 58 JP 1-02, Common Infrastructure – page 93 JP 1-02, National Infrastructure – page 302 JP 1-02.)

Infrastructure Analysis and Assessment. Coordinated identification of DoD, National Defense Infrastructure, and International Defense Infrastructure critical assets, their system and infrastructure configuration and characteristics, and the interrelationships among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets/infrastructures; and assessment of the operational impact of loss or compromise. (CIP Working Definition) (DOD Plan – November 1998)

Infrastructure Protection. Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures (e.g., threat deterrence and vulnerability defense).

Interdependence. Dependence among assets, elements or sites of different infrastructures; therefore, adverse effects incurred against one infrastructure have impact upon the use or availability of another infrastructure. (DoD Plan – November 1998)(NP V 1.0)

Joint Mission Essential Tasking List. A mission task selected by a joint force commander deemed essential to mission accomplishment and defined using the common language of the universal joint task list in terms of task, condition, and

standard. Also called JMET. See also condition, universal joint task list.

Metrics. An agreed-upon measure of performance. (NP V 1.0)

Military Requirement. An established need justifying the timely allocation of resources to achieve a capability to accomplish approved military objectives, missions or tasks. Also referred to as operational requirement. (JP 1-02)

Mission Assurance. Mission assurance encompasses a group of activities that enable or supports all of the foregoing mission areas. Failure to achieve success in any of these area could jeopardize the combatant commands' or the Marine Corps' ability to attain mission success in any or all of it's critical mission responsibilities. (Based upon the U.S. Northern Command Strategic Vision Pamphlet.)

Mission Area Analysis. The CIP Analysis and Assessment process that includes OPLAN/CONPLAN analysis to determine Mission Essential Requirements and critical warfighting assets. The process initiates further infrastructure characterization and assessment to determine dependencies, vulnerabilities, and mission risk.

Mission Critical. Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness and that must be absolutely accurate and available on demand (may include classified information in a traditional context, as well as sensitive and unclassified information). (NP V 1.0)

Mission Essential. Any asset or function that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

Mitigation. A preplanned action or response taken after an event or attack has occurred that is designed to keep mission essential operations, functions and support intact and available for mission execution.

Monitor and Reporting. Indications are preparatory actions or preliminary infrastructure states that signify that an incident is likely, is planned or is underway. An official warning would be issued by the responsible organization.

National Infrastructure. Those infrastructures essential to the functioning of the nation and whose incapacity or destruction would have a debilitating regional or national impact. National infrastructures include telecommunications, electrical power systems, gas and oil transportation and storage, water supply systems, banking and finance, transportation, emergency services and continuity of government operations. (DODD 5160.54) (DOD Plan – November 1998)

National Military Strategy. The art and science of distributing and applying military power to attain national objectives in peace and war. See also Military Strategy, National Security Strategy, Strategy, and Theater Strategy. (JP 1-02, p. 302)

National Security Strategy. The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contributes to national security. Also called national strategy or grand strategy. See also Military Strategy, National Military Strategy, Strategy, and Theater Strategy. (JP 1-02, p. 303)

National Strategy. The art and science of developing and using political, economic, and psychological powers of a nation, together with its armed forces, during peace and war, to secure national objectives. See also strategy. (JP 1-02, p. 303)

Naval Integrated Vulnerability Assessment. An expert third party or peer review comprehensive assessment instrument under DON CIAO coordination and leadership synthesizing several existing assessment protocols including Marine Corps or CNO Integrated Vulnerability Assessments for Antiterrorism and Force Protection (AT/FP); Marine Corps Enterprise Network (MCEN) or Fleet Information Warfare Center (FIWC) assessments for computer network vulnerability; non-organic and other commercial infrastructure assessments performed by Joint Program Office – Special Technology Countermeasures (JPO-STC) or other; and a continuity of operations plans and preparedness assessment under appropriate Navy or Marine Corps community direction. The NIVA s intended to be performed cyclically in all Navy Regions or other major Navy concentration areas, and at major Marine Corps Installations.

Network. Systems with a collection of interconnected nodes. (NP V 1.0)

Operational Impact. Impact of critical assets and OPLANS on other military operations (mobilization, deployment, force projections, etc.)

Operational Impact Analysis. The relationship between military plans and operations and critical assets established through the development of operational dependency matrices and application of operations research methodologies.

Operations Security. The process denying to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities.

Operational Standards/Operational Guidance. Policy, direction, guidance, decision or instruction having the effect of an order when issued by a higher echelon.

Physical Security. (1) That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft. See also Communications Security, Protective Security, Security. (JP 1-02, page 343) (2) Actions taken for the purpose of restricting and limiting unauthorized access; specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks (e.g., through the use of conventional or unconventional weapons). (NP V 1.0)

Presidential Decision Directive/NSC-63. The statement of national intent to protect infrastructures, both cyber and physical, deemed critical to sustainment of the American way of life.

Reconstitution. Refers to actions required to rebuild or restore an aspect or portion of an asset or infrastructure after it has been degraded or destroyed. (DOD Plan – November 1998)

Remediation. Those precautionary actions taken before undesirable events occur to reduce known deficiencies and weaknesses that could cause an outage or compromise a defense infrastructure sector or critical asset. Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc. of critical assets and/or infrastructures, (e.g., emergency planning for load shedding,

graceful degradation and priority restoration); increased awareness, training and education; changes in business practices or operating procedures; asset hardening or design improvements; and system-level changes such as physical diversity, deception, redundancy and back-ups. (NP V 1.0) (CIP Working Definition). (DOD Plan – November 1998)

Response. Response refers to those activities undertaken to eliminate the cause or source of an event. Response activities include coordinated third party (not owner/operator) emergency services (e.g., medical, fire, hazardous or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident.

Risk. The probability that a particular threat will exploit a particular vulnerability of the system (NSA, NCSC Glossary October 1988). The probability of a particular critical asset or infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation.

Risk Analysis or Risk Assessment. The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk Analysis is part of Risk Management (NSA, NCSC Glossary October 1988) produced from the combination of Threat and Vulnerability Assessments characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities.

Risk Management. The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review (NSA, NCSC Glossary, Oct 88). The deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level. Characterized by identifying, measuring and controlling risks to a level commensurate with an assigned value.

Sector. (1) One of two divisions of the economy (private or public); (2) A group of industries or infrastructures, which perform a similar function within a society, e.g. vital human services.

Shared Risk. Refers to risk that, when accepted at a single

Department Activity, subjects all users of interconnected systems and networks to the same risk.

Threat. A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and malicious intent of debilitating the defense or economic security of the United States. A threat may be an individual, organization or nation. (NP V 1.0)

Threat Analysis. A continual process of compiling and examining all available information concerning potential conventional and asymmetric force activities by groups which would target an asset, facility, node, capability or infrastructure. A threat analysis will review the factors of a hostile groups' existence, capability, intentions, history and targeting as well as the security environment within which the friendly forces operate. Threat analysis is an essential step in identifying probability of conventional/asymmetric attack and results in a threat assessment.

Threat Capability. The ability of a suitably organized, trained and equipped entity to access, penetrate or alter government or privately owned information or communication systems and/or to disrupt, deny or destroy all or part of a critical infrastructure. Increased asymmetric threat activity indicates a patchwork of actors that may not individually possess the capability to affect critical capabilities or infrastructures but collectively in loose alliances have increased ability and intent. (National Plan (NP) V 1.0)

Tier Definitions. As determined by the geographic Combatant Commanders in
Chief:

Tier I - Warfighter suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.

Tier II- Sector or element suffers strategic functional failure, but Warfighter strategic mission is accomplished.

Tier III- Individual element failures, but no debilitating strategic mission or core function impacts occur.

Tier IV - Everything else.

Vulnerability. (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system which cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in a unnatural (manmade) hostile environment. (3) In information operations, a weakness in information system security design, procedures, implementation or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 3-07.2 Joint Tactics, Techniques, and Procedures for Antiterrorism – This term and its definition replace the existing term and its definition and are approved for inclusion in the next edition of Joint Pub 1-02.) A characteristic of a critical infrastructure design, implementation or operation of that renders it susceptible to destruction or incapacitation by a threat.

Vulnerability Assessment. Assessment of probability that events will occur using scenario-driven vulnerability index. Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives and verify the adequacy of such measures after implementation.

Vulnerability Metrics. The modeling of actual data supporting vulnerability ratios and indices onto a matrix framework that will show relationships and dependencies of mission, task, function and infrastructure. (JPO-STC)